



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

DES encryption with dummy

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)
[Scholar Help](#)

"with" is a very common word and was not included in your search. [[details](#)]

Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 1,120 for **DES encryption with dummy**

All Results

[H Saputra](#)

[J Wen](#)

[A Fox](#)

[N Vijaykrishna...](#)

[M Kandemir](#)

[Masking the Energy Behavior of DES Encryption - all 17 versions »](#)

H Saputra, N Vijaykrishnan, M Kandemir, MJ Irwin, ... - Proceedings of the conference on Design, Automation and Test ..., 2003 - portal.acm.org

... energy differences due to key-related data- dependent computations in **DES encryption**. ...

An example of such technique involves adding **dummy** modules and activating ...

Cited by 24 - [Related Articles](#) - [Web Search](#)

[Implementation trade-offs of Triple DES in the SRC-6e Reconfigurable Computing Environment - all 5 versions »](#)

OD Fidanci, H Diab, T El-Ghazawi, K Gaj, N ... - Proc. of 2002 MAPLD International Conference - gwu.edu

... The template is completed at runtime when the MAP subprogram's **dummy** arguments become

associated with the actual ... **B. DES Encryption** and Decryption Structure ...

Cited by 12 - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[A format-compliant configurable encryption framework for accesscontrol of video - all 11 versions »](#)

J Wen, M Severa, W Zeng, MH Luttrell, W Jin - Circuits and Systems for Video Technology, IEEE Transactions ..., 2002 - ieeexplore.ieee.org

... block ciphers such as AES and **DES** in the ... Padding with "**dummy**" data for block ciphers

should usually ... identical to the number of codewords before **encryption**. ...

Cited by 74 - [Related Articles](#) - [Web Search](#) - [BL Direct](#)

[Masking the energy behaviour of encryption algorithms - all 6 versions »](#)

H Saputra, N Vijaykrishnan, M Kandemir, MJ Irwin, ... - Computers and Digital Techniques, IEE Proceedings-, 2003 - ieeexplore.ieee.org

... An example of such technique involves adding **dummy** modules and activating them at ...

The core of the **DES encryption** process consists of 16 identical rounds, each ...

Cited by 3 - [Related Articles](#) - [Web Search](#) - [BL Direct](#)

[Clarifying Obfuscation: Improving the Security of White-Box DES - all 3 versions »](#)

HE Link, WD Neumann - ITCC (1), 2005 - doi.ieeecomputersociety.org

... specified, then only that one round of **encryption** will be ... use brute force on a reference

DES implementation to ... we are not concerned with the "**dummy**" T-boxes ...

Cited by 1 - [Related Articles](#) - [Web Search](#)

[Masking the energy behavior of DES encryption \[smart cards\]](#)

H Saputra, N Vijaykrishnan, M Kandemir, MJ Irwin, ... - Design, Automation and Test in Europe Conference and ..., 2003 - ieeexplore.ieee.org



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

dividing with encryption with sequence

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)
[Scholar Help](#)

The following words are very common and were not included in your search: **with**
with. [[details](#)]

Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 20,500 for **dividing with encryption wi**

All Results

[L Qiao](#)

[B Schneier](#)

[X Zhang](#)

[J Tolliver](#)

[R Boyer](#)

[... method and circuit in a receiver of a code division multiple access/direct sequence \(CDMA/DS\) system - all 3 versions »](#)

CY Lee... - US Patent 5,329,546, 1994 - Google Patents

... multiple access/direct **sequence** (CDMA/DS) commu- ... envelope **encryption** and description

techniques with ... **division** multiple access wjiere a digital code is used to ...

Cited by 9 - [Related Articles](#) - [Web Search](#)

[High-speed VLSI architectures for the AES algorithm - all 8 versions »](#)

X Zhang, KK Parhi - Very Large Scale Integration (VLSI) Systems, IEEE ..., 2004 - [ieeexplore.ieee.org](#)

... same **sequence** of transformations as that in the **encryption** structure, and ... However, **dividing** each round unit into arbitrary number of substages does not ...

Cited by 17 - [Related Articles](#) - [Web Search](#)

[Remote auditing of software outputs using a trusted coprocessor - all 16 versions »](#)

B Schneier, J Kelsey - FUTURE GENER COMPUT SYST, 1997 - [schneier.com](#)

... in this protocol are sent protected by **encryption** and **sequence** num- bers ... a keyed one-way hash function instead of an **encryption** function ... 6 **Dividing** the Software ...

Cited by 11 - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[32N+ D bit key encryption-decryption system using chaos - all 3 versions »](#)

JC Magnotti, LA Nelson - US Patent 5,751,811, 1998 - Google Patents

... periodic cryptography, K^K^K; and **encryption-decryption sequence** can be produced with cycle length approaching become- infinity. ...

Cited by 8 - [Related Articles](#) - [Web Search](#)

[A division-of-labor-signature \(t, n\) threshold-authenticated encryption scheme with message linkage ... - all 3 versions »](#)

TS Chen, KH Huang, YF Chung - e-Technology, e-Commerce and e-Service, 2004. EEE'04. 2004 ..., 2004 - [ieeexplore.ieee.org](#)

... of both message linkage and **division** of the ... 7] is a representative authenticated **encryption** scheme with ... Message m consists of the **sequence** } ..., 2 1 t m ...

Cited by 2 - [Related Articles](#) - [Web Search](#)

[Communication method for frequency division multiplexing signalling systems with reduced average ... - all 3 versions »](#)

R Laroia, TJ Richardson, RL Urbanke - US Patent 6,301,268, 2001 - Google Patents

... B the values 0 and 1, the **encryption** operation G ... to recover the original infor- 40 mation **sequence**. ... for transmission by afrequency **division** multiplexing system ...

Cited by 3 - [Related Articles](#) - [Web Search](#)

[A new chaotic algorithm for video encryption - all 7 versions »](#)

same as the **block cipher** used to ... (If it is the same **encryption** algorithm, note ...
Cited by 76 - [Related Articles](#) - [Web Search](#) - [BL Direct](#)

A Proposal for a New Block Encryption Standard - all 7 versions »

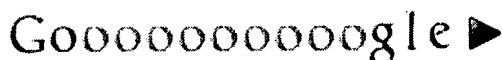
X Lai, J Massey - Proc. EUROCRYPT, 1990 - Springer
... Abstract A new secret-key **block cipher** is proposed as a candidate for a new **encryption stan-** dard. In the proposed **cipher**, the plaintext ...
Cited by 223 - [Related Articles](#) - [Web Search](#)

[PS] High-Bandwidth Encryption with Low-Bandwidth Smartcards - all 24 versions »

M Blaze - Fast Software **Encryption**, 1996 - cerias.purdue.edu
... **encryption** and decryption without the card should be **no** easier than breaking the underlying **cipher**. ... generated by the card for a given **block** should have **no** ...
Cited by 52 - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#)

Hash functions based on block ciphers: a synthetic approach - all 7 versions »

B Preneel, R Govaerts, J Vandewalle - Advances in Cryptology-CRYPTO - Springer
... The **encryption** of plaintext X with key K will be denoted with E(K ... K, C). Unless stated otherwise, it will be assumed that the **block cipher** has **no** weaknesses ...
Cited by 65 - [Related Articles](#) - [Web Search](#) - [BL Direct](#)



Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2007 Google



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

DES with dummy encryption

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)
[Scholar Help](#)

"with" is a very common word and was not included in your search. [[details](#)]

Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 1,090 for **DES with dummy encryption**

All Results

[M Blaze](#)

[H Saputra](#)

[M Akkar](#)

[O Goldreich](#)

[J Wen](#)

[Masking the Energy Behavior of DES Encryption - all 17 versions »](#)

H Saputra, N Vijaykrishnan, M Kandemir, MJ Irwin, ... - Proceedings of the conference on Design, Automation and Test ..., 2003 - portal.acm.org

... energy differences due to key-related data- dependent computations in **DES encryption**.

...

An example of such technique involves adding **dummy** modules and activating ...

[Cited by 24](#) - [Related Articles](#) - [Web Search](#)

[Encryption processing apparatus, encryption processing method, and computer program](#)

R Ochi, S Kusakabe - 2004 - freepatentsonline.com

... which forms the triple-**DES encryption** process as an **encryption** processing unit, sets a **dummy** single-**DES** process as a **dummy encryption** process unnecessary for ...

[Cached](#) - [Web Search](#)

[Masking the energy behavior of DES encryption \[smart cards\]](#)

H Saputra, N Vijaykrishnan, M Kandemir, MJ Irwin, ... - Design, Automation and Test in Europe Conference and ..., 2003 - ieeexplore.ieee.org

... energy differences due to key-related data- dependent computations in **DES encryption**.

...

An example of such technique involves adding **dummy** modules and activating ...

[Related Articles](#) - [Web Search](#)

[The data encryption standard--Retrospective and prospects](#)

R Morris - Communications Magazine, IEEE, 1978 - ieeexplore.ieee.org

... The possibility existed that the **encryption** process might fit on a ... In the latter case, **dummy** biis would be used for ... If for example, the **DES** were to be used in ...

[Cited by 3](#) - [Related Articles](#) - [Web Search](#)

[An implementation of DES and AES, secure against some attacks - all 3 versions »](#)

ML Akkar, C Giraud - Cryptographic Hardware and Embedded Systems-CHES, 2001 - Springer

... insertion of **dummy** instructions; - randomization ... An Implementation of **DES** and **AES**, Secure against Some ... The following timings come from the **encryption** of a 128 ...

[Cited by 87](#) - [Related Articles](#) - [Web Search](#) - [BL Direct](#)

[Countermeasure for Differential Power Analysis using Boolean and Arithmetic masking](#)

W Ng - islab.oregonstate.edu

... first applied to the symmetrical cryptosystems such as **DES encryption** algorithm and ... the differential power attack including of inserting **dummy** code, power ...

[Related Articles](#) - [View as HTML](#) - [Web Search](#)

[A two-phase encryption scheme for enhancing database security - all 4](#)